Autenticación basada en Java card y en certificado X.509 para ambientes universitarios

María Ortega[1] Sergio Sánchez [2]

[1]Universidad Tecnológica de Panamá

[2]Universidad Politécnica de Madrid

maria.ortega2@utp.ac.pa, sergio@diatel.upm.es

Resumen

Este paper presenta la tecnología Java Card y los certificados X.509 como método de autenticación en aplicaciones web en ambientes universitarios, en el caso concreto la Universidad Tecnológica de Panamá (UTP). La solución consiste en mejorar el escenario de acceso a los servicios de la UTP tratando de extender el uso de la Infraestructura de Clave Pública, llevando a cabo la integración de estas tecnologías que aporten mayor seguridad a todos los usuarios y que gozen de un acceso a los servicios ofrecidos de manera flexible, segura, garantizando la autenticidad, confidencialidad, integridad y no repudio.

Abstract

This paper presents the Java Card technology and X.509 certificates as authentication method in web applications in university settings in the specific case the Technological University of Panama (UTP). The solution is to improve the access scenario UTP services trying to extend the use of public key infrastructure, carrying out the integration of these technologies to provide greater certainty for all users and an access services offered in a flexible, secure, ensuring the authenticity, confidentiality, integrity and non repudiation.

1.Introducción

Existen diversos mecanismos de protección de la información que aseguran el cumplimiento de las medidas de seguridad establecidas para el acceso y la utilización de dicha información [Bauer, 2010; Hurtado, 2009]. La autenticación es uno de esos mecanismos y se basa en la identificación de usuarios, es decir, en el proceso mediante el cual se comprueba la identidad de una persona o entidad en base a un conjunto de características [Chávez, 2006].
Atendiendo a qué tipo de características utilizan los sistemas de autenticación para identificar al usuario se pueden clasificar, de forma genérica, en cuatro tipos: los basados en algo que la entidad sabe, los basados en algo que la entidad hace, los basados en algo que la entidad posee y los basados en algo que la entidad es [Hildebrandt et al. 2005; Carracedo, 2004]. Por lo tanto, los sistemas de autenticación comprenden procesos tan simples como el empleo de parejas usuario/contraseña o tan complejos como el análisis de patrones biométricos.

Con los avances tecnológicos y el mayor poder de proceso de los computadores actuales, se da la necesidad de incrementar la seguridad en los procesos de autenticación e incorporar nuevas tecnologías que aumenten y proporcionen un mayor nivel de seguridad. Diversas instituciones cuentan con sistemas de autenticación para el acceso a datos y aplicaciones de autenticación caracterizadas por el uso de usuario/contraseña [Vatra, 2010], denominado acceso clásico, que presentan el problema de que pueden ser fácilmente vulnerados con la tecnología actual,

reduciendo la seguridad de las aplicaciones. Sin embargo, existen otras instituciones que han decidido contar con tecnología más segura a la hora de proteger el acceso a las aplicaciones e información [Diaz et al., 2001; Watts et al., 2010; Harn and Ren, 2011; Watts, J. et al., 2010].
En el caso de estudio concreto abordado en este artículo, el de la Universidad Tecnológica de Panamá (UTP), ésta cuenta con una Infraestructura de Clave Pública (PKI) [Vatra, 2010] utilizada solo por profesores para el registro de calificaciones y por administrativos para la evaluación anual, pero que no está disponible, actualmente, a todos los miembros de la comunidad universitaria.

El objetivo de este trabajo es tratar de mejorar el escenario de acceso a los servicios en la UTP tratando de extender el uso de la PKI [Elfadil and Al-raisi, 2008] y llevando a cabo una integración de tecnologías que aporten mayor seguridad a todos los usuarios (profesores, administrativos y estudiantes) y que garanticen un acceso a los servicios ofrecidos flexible, seguro y con garantías.
En un entorno de uso de clave pública resulta vital asegurarse de que la clave pública que se está utilizando, ya sea para cifra o firmar datos, es en realidad la clave pública adecuada y no una falsificación. Se requiere por lo tanto de un intercambio de información que garantice o demuestre que la clave pública le pertenece al propietario. El mecanismo para garantizar esto es el certificado digital.

El certificado digital es un documento electrónico que demuestra la identidad de un usuario [Network Associates, Inc., 2004] y contiene otros atributos, por ejemplo, las fechas de inicio y fin de la validez del certificado. El certificado digital asocia una clave pública a un usuario y garantiza que la clave es válida y que pertenece al usuario que dice que és quien dice ser. Para ello se designan una o más entidades denominadas Autoridades de Certificación (CAs), cuya función es generar los certificados de clave pública de la organización y luego darlos por buenos. El certificado está firmado por la clave privada (Ks) de la CA y cualquier usuario u organización que pertenece a una red puede verificar con la CA la validez de la clave pública certificada. Las CAs y la administración de certificados digitales utilizan los sistemas de criptografía asimétrica ofreciendo un modelo de confianza que permite construir aplicaciones de alto nivel [Díaz, 2001].
La utilización de criptografía asimétrica [Ramió, 2006] ofrece ventajas como la confidencialidad, para asegurar que ha sido esa persona y no otra la que ha leído o enviado un mensaje; la integridad, para asegurar que el mensaje no podrá ser modificado o alterado; y el no repudio de origen, que imposibilita al usuario negar su participación en una transacción si ha utilizado su firma electrónica puesto que nadie más que él puede haber generado esa firma. Además, la firma permite asegurar la integridad de un documento.

Otro mecanismo de securización que ha tenido una gran aceptación en el mercado actual y está siendo ampliamente utilizado son las tarjetas inteligentes (Smart Cards) [S. C. Allience, 2006]. Ejemplos de uso de este tipo de tarjetas en diferentes ámbitos los encontramos en las tarjetas bancarias de pago seguro o las tarjetas de identificación utilizadas en la administración pública (por ejemplo, el Documento Nacional de Identidad electrónico en España (DNI electrónico, 2010)).
Las tarjetas inteligentes son aquellas que almacenan y procesan información a través de circuitos electrónicos mediante un microcomputador formado por un único chip que se encuentra situado en una tarjeta de plástico típicamente del tamaño de una tarjeta de crédito [Chen, 2000].

Existen diversos tipos de tarjetas inteligentes pero unas de las más interesantes, fundamentalmente por su flexibilidad y fácil adaptación a distintos entornos de utilización, son las tarjetas Java (Java Card). Se trata de tarjetas que utilizan la tecnología Java como base de programación para sus aplicaciones. Se trabaja en Java aplicado a entornos en los que existen ciertas limitaciones en los recursos de memoria, lo que permite la ejecución de pequeñas aplicaciones (applets) escritas en Java dentro del propio microprocesador de la tarjeta, haciendo uso de una máquina virtual Java reducida [Chen, 2000]. Cabe destacar que esta tecnología es compatible con los estándares de tarjetas inteligentes ISO 7816 [ORSI, 2010; Chen, Z. and Di Giorgio, R., 1998].

El resto de éste paper está organizado de la siguiente manera. En la sección 2 se muestra los Trabajos Previos. La sección 3 describe la metodología utilizada en el desarrollo del proyecto. Los Resultados y discusión se encuentran en la sección 4 y finalmente, las conclusiones en la sección 5.

2.Trabajos Previos

La autenticación es el proceso de verificación de identidad de los usuarios y se han realizado una gran cantidad de trabajos brindando solución al problema de autenticación segura, de manera que los usuarios pueden acceder a los servicios y obtener una información confiable. Dentro de los trabajos realizados podemos mencionar el propuesto por Chávez (2006), que sigue los pasos de Anderson (1972) que trabaja en modelos de control de acceso. Chávez, presenta un estudio de mecanismos que regulen la interacción entre los sujetos y objetos, proporcionando autenticación y control de acceso para mayor seguridad de la información. Por otra parte, se presenta el trabajo de Watts (2010) cuyo estudio es ayudar a los estudiantes a entender la necesidad de control de acceso de datos y cómo proteger los datos de la confidencialidad, integridad, autenticación y no repudio mediante el uso de tarjetas inteligentes con PKI para implementar el control de acceso a datos.

Dentro de otros trabajos relacionados tenemos al de Díaz (2001), donde trabaja con algoritmos de cifrado asimétrico y muestra los dos resultados más importantes de esta área: Acero, en el del lado del servidor, y JCCM, en el lado del cliente. Ellos realizaron una red basada en Autoridades de Certificación en relación con el uso de tarjetas inteligentes Java para el almacenamiento de certificados. Otro de los de trabajos relacionados con el desarrollo e implementación de la misma tarjeta java tenemos el de Vossaert (2010), quien cubre los pasos básicos para asegurar el desarrollo de la tarjeta inteligente con la plataforma Java Card.
Por otro lado, otro trabajo relacionado, es el de Harn (2011), quien trabaja con claves y certificado digital, proponiendo el uso de un nuevo concepto llamado Certificado Digital Generalizado (GDC) para la autenticación de usuario y el establecimiento de claves.
También, vemos el trabajo realizado por Henniger (2006), el cual presenta un applet de tarjetas inteligentes que verifica los certificados X.509 almacenados en las tarjetas Java. El enfoque ha sido implementado como un prototipo de funcionamiento de las tarjetas de Java.
A continuación, vemos la metodología empleada en el desarrollo de este proyecto.

3.Metodología del trabajo

La metodología aplicada en la realización de este trabajo consta de varias fases. La primera es la de análisis. En ella se han identificado las necesidad o demandas, los aspectos a mejorar, y se ha realizado un estudio de la situación actual del problema, tomando en cuenta el caso de estudio concreto de la Universidad Tecnológica de Panamá (UTP) que cuenta con una estructura de PKI, utilizada solo por profesores para el registro de calificaciones y por administrativos para la evaluación anual, pero que no está disponible, al día de hoy, a todos los miembros de la comunidad universitaria.

Tras la fase de análisis se ha abordado la fase de diseño. En ella se realiza una propuesta que trata de cubrir las demandas identificadas y de dar solución a todos los problemas y/o carencias detectados en el análisis. Este diseño, desde el punto de vista técnico, consiste en el modelado de una arquitectura lógica a través de diagramas de lenguaje de modelado unificado (Unified Modeling Language - UML).
Como resultado del diseño se presentan modelos desde la vista de componentes que muestran el conjunto de entidades presentes en la arquitectura propuesta como solución y la relación que existe entre ellas. Se aborda también en este punto la integración del certificado X.509 y la tarjeta Java como parte del sistema de autenticación. Así mismo, se presentan dos modelos de comunicación desde la vista de diagramas de secuencia. Uno para la obtención del certificado, es decir, el mecanismo mediante el cual el usuario obtiene un certificado de identidad X.509 que almacena en su tarjeta inteligente y otro correspondiente al acceso a un servicio genérico, es decir, cómo el usuario hace uso de ese certificado para acceder de forma segura y con garantías a los servicios ofrecidos.

Tras el diseño se aborda la fase de implementación. En esta fase se trata de desarrollar un pequeño demostrador de la arquitectura que pueda ser utilizado como implementación de referencia y permita comprobar la funcionalidad de lo diseñado. Sobre este demostrador se realizarán pruebas individuales y, en base a los resultados obtenidos, se volverá a incidir en la fase de diseño para realimentar y mejorar la solución.

4.Resultados y Discusión

En base a la metodología propuesta para este estudio, a continuación se muestra los resultados obtenidos en cada una de las fases.
El certificado digital utilizado en la UTP se puede descargar y puede ser portado en un dispositivo extraíble como un token, una tarjeta, etc., pero en la actualidad no se cuenta con la posibilidad de tener estos dispositivos. El certificado digital se encuentra en un repositorio de manera que cuando los profesores y administrativos (actuando a modo de clientes) lo necesitan para firmar algo, es la aplicación web (que actúa como proveedora de servicio) la que llama o hace la búsqueda en el repositorio para su utilización. En este escenario no está involucrado todo el personal de la universidad que accede a los recursos ofrecidos por la UTP. Por ejemplo, los estudiantes ingresan y realizan sus solicitudes al sistema de matrícula, al correo o a los cursos virtuales por medio de un sistema de autenticación basado en usuario/contraseña. El estudiante dispone por lo tanto de múltiples credenciales para ingresar a cada uno de esos servicios, en términos generales de una pareja usuario/contraseña por servicio.

Como resultado del análisis se ha detectado la necesidad de un escenario donde se involucre a todo el personal de la UTP, es decir, un escenario global. Cada uno de los miembros de la Universidad accederá a sus aplicaciones de acuerdo a su rol de forma segura y cómoda.
También se ha identificado la necesidad de emplear comunicaciones seguras basadas en cifrado y autenticación, en las que existan garantías de origen, confidencialidad, integridad y no repudio. Adicionalmente se busca que el acceso de los usuarios sea cómodo y el elemento de autenticación, además de seguro, sea portable, es decir, que los miembros de la Universidad puedan llevar su identidad con ellos para acceder a los distintos servicios desde el lugar donde se encuentren, pero siempre garantizando el transporte seguro de los tokens de identidad, la confidencialidad, la autenticidad y el no repudio.

En base a lo anterior se propone la utilización de algoritmos de clave asimétrica tal como RSA y los mecanismos de cifrado y firma digital para cubrir las necesidades de una comunicación segura en la que se proporcione confidencialidad, integridad de los datos, garantía de origen y no repudio. Como mecanismo de gestión de las claves se propone la utilización de la PKI y el certificado X.509, que asocia la clave con la identidad de la persona.
Como mecanismo de almacenamiento y transporte de las claves y certificados se propone la utilización de las tarjetas Java por todo el personal que participa en la universidad. La razón está en su comodidad y en que proporcionan la interoperabilidad, seguridad, portabilidad, capacidad para múltiples aplicaciones y compatibilidad con los estándares existentes de tarjetas inteligentes.

A partir de lo expuesto en los párrafos anteriores se han identificado los distintos componentes involucrados en el escenario. Son los siguientes:

- Usuario: persona que va a hacer uso de algún servicio ofrecido por la UTP. Puede ser administrativo, profesor o estudiante.
- Proveedor de servicios: Institución que proveerá los servicios para los usuarios. En este caso en concreto es la UTP.
- PC: dispositivo desde el que el usuario va acceder al servicio. El usuario puede hacer uso del PC desde la institución o desde la comodidad de su hogar.
- Lector de tarjeta Java: Estará conectado al PC y se comunicará con él. Leerá la tarjeta Java.
- Tarjeta Java: Almacena las claves y certificados de identidad del usuario. A través del lector se comunica con las aplicaciones necesarias y gestiona el control de acceso al usuario y el uso del certificado para acceder a las aplicaciones o servicios ofrecidos por la institución.
- PKI: infraestructura de clave pública que estará asociada a la UTP y que será encargada de entregar los certificados a los usuarios. Constará de una Autoridad de Registro (RA) para validar el registro de usuario y de una CA para emitir y consultar el estado del certificado X.509 de un usuario.

Con todas estas entidades, se presenta a continuación la arquitectura lógica de la solución, recogida en la figura 1. En ella se identifican los componentes para la arquitectura de comunicación, las entidades participantes y la relación que existe entre ellas.

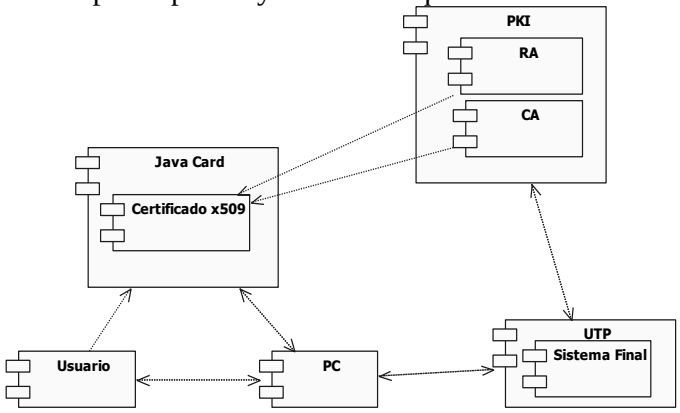

Figura 1. Arquitectura lógica y relaciones

El usuario dispone de una tarjeta Java que comunica con el PC, por medio del lector de tarjetas Java, para hacer uso de algún servicio ofrecido por la institución. Se realiza una primera fase de autenticación del usuario basada en un Número de Identificación Personal (PIN) para comprobar que es el propietario de la tarjeta. Para acceder al servicio se toma en cuenta la PKI asociada a la institución, que es la encargada de emitir los certificados a los usuarios con ayuda de la CA y la RA. Para ello, el usuario se autentica mediante el certificado que está almacenado en la tarjeta Java y accede al sistema final. En la figura 2 se presenta la arquitectura de la comunicación de la tarjeta Java con el lector de tarjetas o CAD (Card Accepting Device). El intercambio de información y comandos entre la tarjeta y el CAD se realiza a través de Unidades de Datos del Protocolo de Aplicación o APDUs (Application Protocol Data Units). Las APDUs son paquetes de información con un formato específico, de acuerdo al estándar ISO 7816 [6, 23-24]. Se definen dos tipos de APDU, los Command APDU, que son los que se envían hacia la tarjeta, y los Response APDU, que son los que se envían desde la tarjeta como respuesta a un Command APDU.

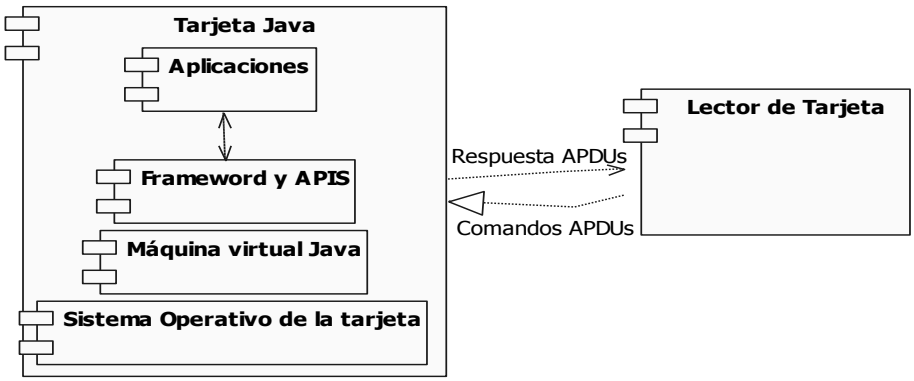

Figura 2. Comunicación de la tarjeta y el CAD

Con la intención de obtener una visión clara de los intercambios de datos que tienen lugar se presentan a continuación los diagramas de secuencia de los dos casos de uso que los autores consideran más importantes: la obtención del certificado de identidad por parte de un usuario y el acceso a un servicio. En la figura 3 se presenta el diagrama de secuencia primero, el correspondiente a cómo el usuario obtiene el certificado digital de identidad X.509 y cómo dicho certificado se almacena en su tarjeta inteligente.

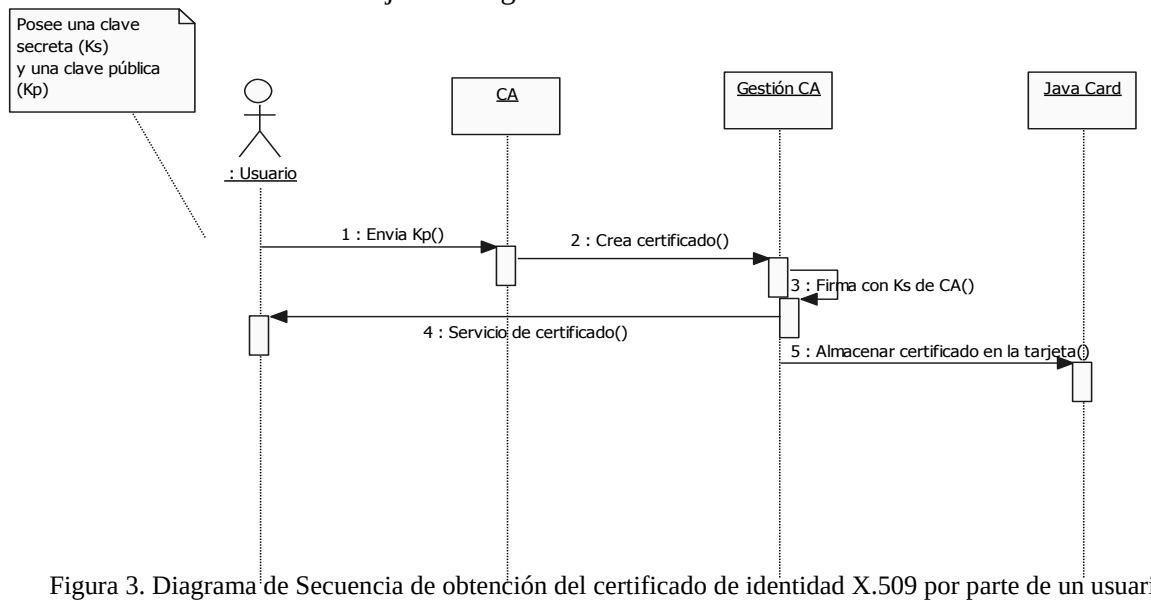

Figura 3. Diagrama de Secuencia de obtención del certificado de identidad X.509 por parte de un usuario

El usuario posee su clave pública (Kp) y su clave secreta (Ks), generadas previamente por algoritmos criptográficos, pero necesita contar de una tercera parte de confianza (TTP) como la RA, para que valide el registro de usuario y de la CA, que es la entidad que permite emitir y consultar el estado de un certificado X.509. Para la obtención del certificado, el usuario envía su Kp a la CA, ésta realiza el proceso de emisión del certificado y firma con su propia clave secreta para que conste que ese certificado es válido ante todo los miembros de ese entorno. La Kp del usuario es dada a conocer a todos, mientras su Ks es privada, solo la debe conocer el usuario dueño del certificado. Es importante mencionar que se parte del supuesto de que es imposible obtener la Ks a partir de la Kp.

Una vez emitido el certificado, la Ks es almacenada dentro de la tarjeta Java y la Kp dentro del certificado digital que estará almacenado en la tarjeta Java para mayor seguridad para luego ser utilizado en el acceso a cualquier servicio que necesite el usuario. Por lo tanto, el usuario posee en sus manos un servicio de autenticación portable, seguro y flexible.
Por otra parte, se ha realizado el diagrama de secuencia correspondiente al acceso a un servicio. En él se muestra cómo el usuario accede a los servicios autenticándose y utilizando la seguridad del certificado digital X.509 almacenado en su tarjeta inteligente (ver Figura 4).

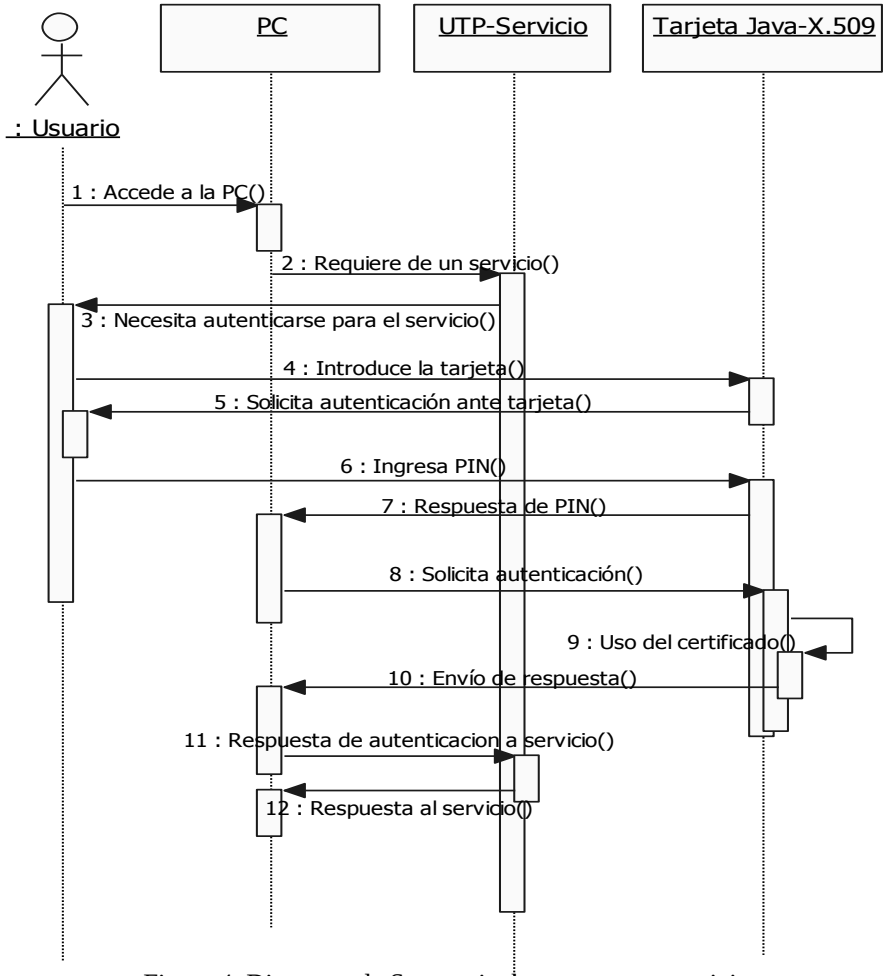

Figura 4. Diagrama de Secuencia de acceso a un servicio

El usuario desde la comodidad donde se encuentre accede al PC para hacer uso de un servicio ofrecido por la institución. Necesita autenticarse para acceder a dicho servicio e introduce su tarjeta Java que a su vez le solicita autenticación para comprobar que es el dueño de la tarjeta.

El usuario ingresa su PIN para la tarjeta y se realiza la autenticación del usuario ante la tarjeta, obteniéndose una respuesta a la solicitud. El usuario se ha identificado ante la tarjeta como paso previo a la posibilidad de autenticarse para acceder al servicio. En esta segunda autenticación, la de acceso propiamente al servicio, se utiliza el certificado digital X.509 almacenado en la tarjeta que demuestra la identidad del titular ante cualquiera mediante un mecanismo de, por ejemplo, reto-respuesta en el que intervengan tanto la Kp como la Ks del usuario, ambas almacenadas en su tarjeta. De esta manera se autentica el usuario y puede acceder de forma segura al sistema final.
Una vez presentados globalmente los resultados de la fase de diseño se aborda a continuación la fase de implementación, en la que se consideran tres partes. La primera trata el desarrollo del módulo de autenticación básica. La segunda corresponde a la integración del certificado X.509 de identidad en la tarjeta Java y la tercera comprende el desarrollo del módulo de la aplicación final, que consiste en un pequeño demostrador para comprobar la funcionalidad de la solución planteada.

Para realizar pruebas de la autenticación básica utilizando la tarjeta Java, se ha desarrollado una aplicación de prueba que ha permitido validar los supuestos planteados conceptualmente utilizando el emulador para tarjeta Java 3.0 integrado en el entorno integrado de desarrollo Netbeans. La aplicación desarrollada consta de tres funciones principales: la autenticación, la verificación del estado (autenticado o no) y el reseteo y desbloqueo de la cuenta de usuario almacenada en la tarjeta.
Para establecer los parámetros necesarios para definir el esquema de autenticación basado en las tarjetas Java es indispensable definir los comandos (Command APDUs) que representan las funcionalidades y constantes requeridas para realizar la autenticación basada en contraseñas (PIN). Uno de los principales aspectos a recalcar de este procedimiento es la posibilidad de incluir contraseñas de longitud variable.
En las pruebas realizadas se utilizó un array de bytes como representación de la contraseña de usuario que debe ser incluido en la APDU utilizada para realizar la autenticación. También se definieron constantes para representar el límite de intentos permitidos para el acceso a la tarjeta, los códigos de errores y las APDU de respuesta a una acción específica.
Con ello se ha comprobado el funcionamiento de la tarjeta Java y el del lector de tarjetas inteligentes.

Una vez comprobado el mecanismo de autenticación básica ante la tarjeta se procede a la integración del certificado digital X.509 en la misma.
Para la integración del certificado en la tarjeta es necesario un proceso previo de generación de la clave pública a certificar y la clave privada asociada. Para ello se ha utilizado un conjunto de clases Java y algoritmos criptográficos que se invocan y ejecutan dentro de la propia tarjeta Java, garantizándose de este modo que la Ks nunca sale de la tarjeta y se mantiene en un dispositivo de almacenamiento seguro durante todo su ciclo de vida.
Una vez obtenidas las claves se procede a la generación del certificado digital X.509 asociado a la Kp generada. Previamente y en este caso en concreto se ha procedido a la creación de una CA propia dentro de la institución y será ella la que se encarge de la creación del certificado.
Una vez se cuenta con una CA y tras demostrar su identidad ante la RA asociada, el usuario solicita su certificado digital para su Kp. La CA emite un certificado digital de identidad basado en el estándar X.509 que consiste en versión, número de serie, algoritmo, nombre del emisor del certificado, periodo de validez de dicho certificado y clave pública que certifica (en este caso Kp del usuario) entre otros.
Dentro del entorno de la institución, la clave pública del usuario es dada a conocer a todos los miembros y el usuario mantendrá en privado su Ks.

5.Conclusiones

Para el desarrollo de este trabajo se ha utilizado una metodología basada en varias fases, comenzando con el análisis de requisitos y llegando hasta la implementación y pruebas de parte de lo diseñado.

Como se ha visto a lo largo del texto, se parte del estudio del caso concreto de la UTP, donde la autenticación para algunos usuarios se basa en certificados digitales de identidad almacenados de forma centralizada y para otros en el sistema clásico de usuario y contraseña. El cual, por su propia constitución resulta un poco inapropiado, ya que se requiere mayor seguridad en la institución.

De igual manera, se hace necesario involucrar a todo el personal en general que requiere de los servicios ofrecidos por la institución, pero manteniendo una comunicación segura. En este artículo se propuso la utilización de la criptografía asimétrica que proporciona medios para asegurar la comunicación y el uso de la tecnología Java.

La solución se basa en el uso de PKI para el acceso a los servicios ofrecidos por la institución, utilizando algoritmos asimétricos para la creación de las claves del usuario. Se ha creado una infraestructura de seguridad que está compuesta por CA y RA que son las entidades encargadas de la generación y registro de los certificados digitales utilizados por los usuarios de acuerdo a su rol. Además se ha incluido el uso de tarjetas Java para el almacenamiento del certificado y autenticación del usuario. La flexibilidad, practicidad y comodidad son algunas de las ventajas que ofrece esta tecnología.

Para comprobar la funcionalidad de lo diseñado, se ha desarrollado un pequeño demostrador de usuario/servidor o implementación de referencia. Se hace mención que es a pequeña escala, para futuras ampliaciones. Este consiste en el almacenamiento del certificado X.509 en la tarjeta Java y de una aplicación para acceder al recurso mediante la autenticación de la tarjeta y luego del certificado del usuario.

Con la integración de las dos tecnologías, se ha obtenido los beneficios de cada una como mayor escalabilidad, portabilidad, interoperabilidad y seguridad de la información en las aplicaciones.

Esto ha permitido una comunicación más segura que garantiza la autenticidad, la confidencialidad, la integridad y el no repudio de origen que es un punto importante porque es un servicio de seguridad que permite probar la participación de un usuario o entidad en una comunicación.

Como trabajo futuro, se pretende mejorar el acceso a la tarjeta Java mediante identificación biométrica, la cual dará mayor seguridad al momento de autenticarse.

Referencias

[Bauer, 2010] Bauer, L., et al., (2010). Constraining Credential Usage in Logic-Based Access Control. Proceding of the 2010 23rd IEEE Computer Security Foundations Symposium (CSF), Edimburgo, Escocia, pp. 154-168.

[Carracedo, 2004] Carracedo, J. (2004). Seguridad en redes telemáticas. McGraw-Hill, Madrid, España.

[Chávez, 2006] Chávez, P. (2006). Autenticación y Control de Acceso. http://lsc.fie.umich.mx/~pedro/autenticacion_ac.pdf

[Chen, 2000] Chen, Z. (2000). Java Card™ Technology for Smart Cards: Architecture and Programmer's Guide. Addison-Wesley, California, USA.

[Chen, 1998] Chen, Z. and Di Giorgio, R., InfoWorld JavaWorld, Solutions for java Developers, Understanding Java Card 2.0. http://www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev.html
[Díaz, 2001] Díaz, I. et al. (2001). Autenticación en la Red: ACerO y JCCM*: Java Card Certicate Management. III Jornadas de Ingeniería Telemática. JITEL. Barcelona, España, pp. 405-412.
[DNI electrónico, 2010] DNI electrónico, Guía de Referencia Básica, v1.3, 2010. http://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1_3.pdf
[Elfadil, 2008] Elfadil, N. A. et al. (2008). An Approach for Multi Factor Authentication for Securing Smart Cards' Applications. Proceedings of the International Conference on Computer and Communication Engineering IEEE. Kuala Lumpur, Malasia, pp. 368-372.
[Harn, 2011] Harn, L. and Ren, J., 2011. Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications. IEEE Transactions on Wireless Communications. Vol. 10, No. 7, pp. 2372 – 2379.
[Henniger, 2006] Henniger, O. et al. Verifying X.509 Certificates on Smart Cards. In proceeding World Academy of Science, Engineering and Technology 22 2006.
[Hilderbart, 2005] Hildebrandt, M. Et al. (2005). Future of Identity in the Information Society. FIDIS Inventory of Topics and Clusters, Deliverable 2.1, pp 38-39 [online] Disponible en: http://www.cosic.esat.kuleuven.be/publications/article-829.pdf
[Hurtado, 2009] Hurtado, D. et al., 2009. Modelado de la seguridad de objetos de aprendizaje. Generación Digital, Vol. 8, No. 1. pp. 38-42.
[ISO, 2011] International Organization for Standardization (ISO). International Standard. Identification Cards-Integrated circuit cards. ISO/IEC 7816-1:2011(E). http://webstore.iec.ch/preview/info_isoiec7816-1%7Bed2.0%7Den.pdf
[Netvork Associates, 2004] Network Associates, Inc. and its Affiliated Companies, 2004. An Introduction to Cryptography. Network Associates, Inc. California, USA.
[Ramió, 2006] Ramió, J., 2006. Libro Electrónico de Seguridad Informática y Criptografía. http://www.criptored.upm.es/descarga/SegInfoCrip_v41.zip
[S.C.Alliance, 2006] S. C. Allience, 2006, Uso de tarjetas inteligentes para un control de acceso físico seguro, Informe de la Smart Card Alliance Latin America (SCALA). http://www.smartcardalliance.org/latinamerica/translations/Secure_Physical_Access_Spanish.pdf
[ORSI, 2010] Observatorio Regional de la Sociedad de la Información de Castilla y León (ORSI), Tarjeta ciudadana, una visión de las tarjetas inteligentes y su aplicación en los ayuntamientos, 2010.http://www.jcyl.es/web/jcyl/binarios/910/900/TARJETA_CIUDADANA.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8
[Vatra, 2010] Vatra N. (2010). Public Key Infrastructure for Public Administration in Romania. Communications (COMM), 2010 8th International Conference, IEEE. Bucarest, Rumania, pp. 481-484.
[Vossaert, 2010] Vossaert, J. (2010). Developing secure Java Card applications.
[Watts, 2010] Watts, J.et al., 2010. Case Study: Using Smart Cards with PKI to Implement Data Access Control for Health Information Systems. Proceding of the IEEE SoutheastCon 2010 (SoutheastCon). Concord, NC, USA, pp. 163-167.